

CLAIMS

What is claimed is:

1. A method for administering portal security for an object, comprising the steps of:
5 extracting a native security setting from a native environment of the object;
mapping the native security setting into a portal security setting associated with a portal; and
associating in the portal said portal security setting with the object.
- 10 2. The method of claim 1, the native security settings comprising an identity of an entity external to the portal having a predetermined security relationship with the object in its native environment, the portal comprising a metadata object corresponding to the object, further comprising the steps of:
mapping the external entity into a corresponding portal entity; and
15 instantiating the predetermined security relationship between the metadata object and the corresponding portal entity.
3. The method of claim 2, wherein said predetermined security relationship is viewing access.
20
4. The method of claim 2, the native security settings comprising identities of external users and external groups having the predetermined security relationship with the object in its native environment, further comprising the steps of:
mapping the external users and external groups into corresponding portal users and
25 groups according to a predetermined mapping process; and
associating the corresponding portal users and portal groups with the object according to the predetermined security relationship.
5. The method of claim 4, wherein said predetermined mapping process is executed
30 according to information maintained in a portal database.

6. The method of claim 5, wherein said information maintained in the portal database comprises:

portal user and portal group information including membership information relating the portal users to portal groups; and

5 a first synchronization map that maps external domains to an intermediate set of domain identifiers; and

a second synchronization map that maps external groups to an intermediate set of group identifiers.

10 7. The method of claim 6, wherein said portal users are identified by a concatenation of a portal domain identifier and a user name used by the external domain of the user, and wherein said portal groups are identified by a concatenation of a portal domain identifier and a group name used by the external domain of the group.

15 8. The method of claim 7, said predetermined mapping process comprising the steps of:

forming a reflexive set of external users and external groups having access to the object, each member of the reflexive set being expressed as a concatenation of the external domain and the external user or external group;

20 mapping each external domain indicated in each of the external users and external groups into to one or more portal domains using the first synchronization map;

mapping each external group to one or more portal simple group names using the second synchronization map;

forming a candidate set of all possible pairings between (i) all indicated external
25 and portal domains, and (ii) all indicated external group and portal simple group names;

comparing the candidate set to said portal user and portal group information; and

deleting from the candidate set any member not appearing in said portal user and portal group information;

wherein the remaining members of the candidate set represent the corresponding
30 portal users and portal groups having access to the object.

9. A corporate portal system, comprising:
a crawler for accessing external objects in external domains;
a security extraction utility for extracting native security information corresponding to the external objects from one or more security systems of the external domains; and
5 a database comprising information for mapping the extracted native security information into a security system of the corporate portal;
wherein the security system of the corporate portal regulates exposure of portal metadata objects corresponding to the external objects based on the mapped security information.
- 10
10. The corporate portal system of claim 9, further comprising a synchronization agent for accessing external user and external group information from the external domains, wherein said database comprises information derived at least in part from said external user and external group information.
- 15
11. The corporate portal system of claim 10, further comprising an administrative user interface for assisting a portal administrator in populating said database using information that includes said external user information and said external group information.
- 20
12. The corporate portal system of claim 11, wherein said synchronization agent is adapted and configured to extract user and group information from external domains having directory types of: Windows NT, LDAP, or ODBC.
- 25
13. A computer program product for use in administering portal security for an object, comprising:
computer code for extracting a native security setting from a native environment of the object;
computer code for mapping the native security setting into a portal security setting associated with a portal; and
30 computer code for associating in the portal said portal security setting with the object.

14. The computer program product of claim 13, the native security settings comprising an identity of an entity external to the portal having a predetermined security relationship with the object in its native environment, the portal comprising a metadata object

5 corresponding to the object, further comprising:

computer code for mapping the external entity into a corresponding portal entity;
and

computer code for instantiating the predetermined security relationship between the metadata object and the corresponding portal entity.

10

15. The computer program product of claim 14, wherein said predetermined security relationship is viewing access.

16. The computer program product of claim 14, the native security settings comprising
15 identities of external users and external groups having the predetermined security relationship with the object in its native environment, further comprising:

computer code for mapping the external users and external groups into
corresponding portal users and groups according to a predetermined mapping process; and
computer code for associating the corresponding portal users and portal groups

20 with the object according to the predetermined security relationship.

17. The computer program product of claim 16, wherein said predetermined mapping process is executed according to information maintained in a portal database.

25 18. The computer program product of claim 17, wherein said information maintained in the portal database comprises:

portal user and portal group information including membership information relating the portal users to portal groups; and

a first synchronization map that maps external domains to an intermediate set of
30 domain identifiers; and

a second synchronization map that maps external groups to an intermediate set of group identifiers.

19. The computer program product of claim 18, wherein said portal users are identified
5 by a concatenation of a portal domain identifier and a user name used by the external domain of the user, and wherein said portal groups are identified by a concatenation of a portal domain identifier and a group name used by the external domain of the group.

20. The computer program product of claim 19, said computer code for mapping the
10 external users and external groups into corresponding portal users and groups according to a predetermined mapping process comprising:

computer code for forming a reflexive set of external users and external groups having access to the object, each member of the reflexive set being expressed as a concatenation of the external domain and the external user or external group;

15 computer code for mapping each external domain indicated in each of the external users and external groups into to one or more portal domains using the first synchronization map;

computer code for mapping each external group to one or more portal simple group names using the second synchronization map;

20 computer code for forming a candidate set of all possible pairings between (i) all indicated external and portal domains, and (ii) all indicated external group and portal simple group names;

computer code for comparing the candidate set to said portal user and portal group information; and

25 computer code for deleting from the candidate set any member not appearing in said portal user and portal group information, wherein the remaining members of the candidate set represent the corresponding portal users and portal groups having access to the object.